Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of updating mobile electronic devices, the method comprising:

informing a notification history server of notifications sent by various ~~authorized~~ senders of updates to a mobile electronic device, the notification history server keeping a record of ~~authorized~~ all verified and unverified notifications, the notification history server being distinct from the various ~~authorized~~ senders of updates and distinct from a device management server managing the mobile electronic device;

receiving a notification in ~~an~~ the mobile electronic device that an update is available from a particular sender;

determining authorization ~~authenticity~~ of the received notification in the mobile electronic device by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining, by comparison, whether the notification history server has [[a]] previous verified or unverified records of the notification from the particular sender using the information sent by the electronic device thereby avoiding testing of each notification; ~~and~~

the mobile electronic device downloading the available update from the particular sender if the notification history server confirms having the verified record of notification from the particular sender ~~knowledge~~ of the notification; and

the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification.

2. (Previously Presented) The method according to claim 1, further comprising:

simultaneously informing the notification history server that the notification has been sent to the electronic device.

3. (Cancelled).

4. (Currently Amended) The method according to claim 1, further comprising:

ignoring the notification in the electronic device upon determining that the notification is unverified ~~inauthentic~~;

recording that an unverified ~~inauthentic~~ notification has been received; and

waiting to receive another notification in the electronic device.

5. (Currently Amended) The method according to claim 1, further comprising determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is verified ~~authentic~~.

6. (Original) The method according to claim 5, further comprising:

retrieving the update package; and

performing an update of at least one of firmware and software resident in the electronic device.

7. (Original) The method according to claim 1, wherein the notification comprises one of a short message service (SMS) notification, an instant messaging

(IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

8. (Original) The method according to claim 1, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

9. (Currently Amended) The method according to claim 1, wherein determining the authorization ~~authenticity~~ of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server.

10. (Original) The method according to claim 9, wherein an authorized server comprises one of a management server and a customer care center.

11. (Original) The method according to claim 1, wherein the notification comprises location and identification information regarding a management server providing access to an update package and information regarding the update package.

12. (Original) The method according to claim 11, wherein location and identification information comprise at least one of a universal resource locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

13. (Original) The method according to claim 1, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event.

14. (Currently Amended) The method according to claim 13, wherein retrieving the update package from the default management server is performed after authorization ~~authentication~~ of the notification message.

15. (Original) The method according to claim 1, further comprising:

retrieving an update package via a download agent in the electronic device; and

updating at least one of firmware and software in the electronic device via an update agent in the electronic device.

16. (Original) The method according to claim 1, further comprising preventing unauthorized updates of at least one of firmware and software in the electronic device.

17. (Currently Amended) The method according to claim 16, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authorization ~~authenticity~~ of the notification, and abort the update process if the notification is determined to be unverified ~~inauthentic~~, and permit the update package to be downloaded, if the notification is determined to be verified ~~authentic~~.

18. (Original) The method according to claim 16, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

19. (Original) The method according to claim 1, further comprising provisioning an address of a management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

20. (Currently Amended) A mobile services network at least comprising:

at least one mobile electronic device;

a device management server communicatively linked with the at least one mobile electronic device via a communication link for managing the at least one mobile device; and

a notification history server distinct from the device management server and operatively connected to the management server, the notification history server comprising a record of all verified ~~authentic~~ notifications and unverified notifications sent to the at least one mobile electronic device by various ~~authorized~~ senders, the various ~~authorized~~ senders being distinct from the notification history server, wherein the notification history server is able to determine authorization of an available update by comparing whether the notification history server has previous verified or unverified records of notification from a particular sender thereby avoiding testing of each notification;

wherein the mobile electronic device is adapted to:

receive notifications as to available updates to firmware on the mobile device;

send information retrieved from the notifications to the notification history server;

download available updates associated with notifications sent to the notification history server for which the notification history server has a previous verified record from the particular sender; and

ignore available updates associated with notifications to the notification history server for which the notification history server has a previous unverified record from the particular sender ~~determine the authenticity of a notification received from a sender by contacting the notification history server and determining whether the notification history server has a record, from one of the authorized senders, of the notification received by the electronic device~~.

21. (Original) The network according to claim 20, wherein the electronic device at least comprises:

non-volatile memory;

a short message entity;

random access memory; and

security services.

22. (Original) The network according to claim 21, wherein the non-volatile memory in the electronic device at least stores:

an update agent;

a firmware and real-time operating system;

an operating system layer;

a download agent or browser; and

an end-user related data and content.

23. (Original) The network according to claim 20, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

24. (Previously presented) The network according to claim 20, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server.

25. (Currently Amended) The network according to claim 24, wherein the notification history server is adapted to determine whether a notification is authorized ~~authentic~~ by examining message identification information in the notifications.

26. (Currently Amended) The network according to claim 24, wherein the electronic device is adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authorized authentic.

27. (Original) The network according to claim 24, wherein the electronic device is adapted to determine whether a notification originated from an authorized sender.

28. (Original) The network according to claim 27, wherein an authorized sender is at least one of the management server and a customer care center resident in the network.

29. (Original) The network according to claim 20, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages.

30. (Original) The network according to claim 20, wherein notifications comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol

(WAP) push message notification, and an enhanced messaging service (EMS) notification.

31. (Original) The network according to claim 30, wherein notifications further comprise at least one user data field containing message identification information.

32. (Original) The network according to claim 30, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package.

33. (Original) The network according to claim 32, wherein location and identification information comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

34. (Currently Amended) The network according to claim 20, wherein upon determining that a notification received in the electronic device is unverified ~~inauthentic~~, the electronic device is adapted to ignore the notification and wait for another notification, and a record is created recording that an unverified ~~inauthentic~~ notification has been received.

35. (Original) The network according to claim 20, wherein the management server comprises the notification history server and an update package repository.

36. (Original) The network according to claim 20, wherein the notification history server is incorporated into a short message center in the network.

37. (Original) The network according to claim 20, further comprising a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device.

38. (Currently Amended) The network according to claim 37, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authorization ~~authenticity~~ of the notification, and abort the update process if the notification is determined to be unverified ~~inauthentic~~, and permit the update package to be downloaded, if the notification is determined to be verified ~~authentic~~.

39. (Original) The network according to claim 37, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

40. (Original) The network according to claim 20, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification. the notification comprising server address information, and wherein the electronic device is adapted

to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.